IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

JUNIPER NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. 11-1258-SLR
	)	
PALO ALTO NETWORKS, INC.,	)	
	)	
Defendant.	)	
	)	
	)	

DEFENDANT PALO ALTO NETWORKS, INC.'S OPENING BRIEF IN SUPPORT OF ITS MOTION FOR SUMMARY ADJUDICATION OF ANTICIPATION AND OBVIOUSNESS FOR THE '612 AND '347 PATENTS

Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
POTTER ANDERSON & CORROON LLP
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

Attorneys for Defendant Palo Alto Networks, Inc.

OF COUNSEL:

Harold J. McElhinny
Michael A. Jacobs
Matthew I. Kreeger
Matthew A. Chivvis
Morrison & Foerster LLP
425 Market Street
San Francisco, CA 94105-2482
(415) 268-7000

Daralyn J. Durie
Ryan M. Kent
Durie Tangri LLP
217 Leidesdorff Street
San Francisco, CA 94111
(415) 362-6666

Dated: August 20, 2013

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

I. INTRODUCTION

Although the asserted patents purport to describe narrow improvements over the prior art, Juniper Network Inc.'s ("Juniper") litigation approach has been to seek broad interpretations of the claims. But Juniper's proposed constructions are so broad that they would render the claims invalid in view of the prior art. By its motion, Palo Alto Networks, Inc. ("PAN") shows that under Juniper's reading of the claims, prior art anticipates or renders obvious two of the patents at issue: U.S. Patent Nos. 7,107,612 and 6,772,347. That the asserted claims from these patents were disclosed in the prior art turns not on disputed facts or interpretations of the prior art references, but rather is apparent from a review of the references themselves. Summary adjudication of anticipation and obviousness is therefore appropriate for these two patents.

II. BACKGROUND

The '612 patent is a continuation of the '347 patent, which in turn is a continuation-in-part of U.S. Patent No. 6,701,432. Hence, the earliest possible priority date for the '612 and '347 patents can be no earlier than the filing date for the '432 patent, which is April 1, 1999.[1] The '612 patent is the subject of an Inter Partes Review request at the PTO, while an Inter Partes Reexamination request as to the '347 patent was recently denied. Neither of these two patents is subject to the Court's order regarding assignor estoppel (ECF No. 53), and none of the named inventors is currently employed by PAN. As discussed below, under at least Juniper's interpretation of the '612 and '347 patent's claims, they are anticipated and rendered obvious by prior art with dates before the earliest possible priority date for these patents.

[1] PAN disputes whether the '612 and '347 patents are entitled to priority to the '432 patent's filing date based on the substantial new matter that was included in the '347 patent, but priority does not affect PAN's motion as the prior art relied upon pre-dates the earliest possible priority date.

The ’612 and ’347 patents are both directed to improved firewalls. The ’612 patent claims a dynamic filter which adds or modifies rules based on data extracted from received packets, and the ’347 patent claims a two-step filtering process where initially denied packets are further sorted to determine whether they should be allowed or denied.

Packet switching — allowing computers to communicate over a network using discrete “packets” of data that can be routed to a destination — has been known in the art at least since the 1960s. In a conventional network, each packet has a sender address and a receiver address. Packets also typically contain other descriptive information in a section called the packet header and data in a section called the payload. Networking devices communicate using well-known protocols that consist of rules for transferring packets and processing packet data formats associated with them. (Mitchell Decl. ¶¶ 39-44.)

An important aspect of communications protocols is the “layers” model. To send a file that is divided into a set of packets, specific network protocols are used to transfer packets from one computer to another. At the transport layer, a protocol such as Transport Control Protocol (“TCP”) divides a message or portions of a message into packets, numbers those packets, and ensures that all packets sent are also received. TCP routes the communications by using Internet Protocol (“IP”) addresses and port numbers. The IP addresses are used by the network layer to identify the locations of the sending and receiving computers, while port numbers are used to identify a particular process at each end point to which the packets should be delivered. (*Id.* ¶¶ 46-53.)

As the popularity of the Internet grew, protecting computers connected to a public network (such as the Internet) from unauthorized access became more important. One simple way to protect computers on a private network is to insert a firewall between the private network and the public network. As described in the shared specification of the ’612 and ’347 patents,

prior art firewalls protect the private network from unauthorized access by screening or filtering data packets at the boundary or interface of the private and public networks. (*See, e.g.*, '612 Patent at Fig. 1; 1:51-61.) A firewall operates by passing only authorized traffic, as defined by some security policy (which is referred to as an access control policy (*see id.* at 2:16-19)), from one network to the other. A security policy may allow or prevent communication based on a number of rules. (*See id.* at 2:38-65.)

The patents acknowledge that firewalls with fixed sets of access rules were well known before the effective filing date of the '612 and '347 patents. (*See, e.g., id.* at 2:38-3:2; *see also* Mitchell Decl. ¶¶ 56-61.) A simple firewall with a fixed set of rules for filtering packets is also known as a "static packet filter." (Mitchell Decl. ¶ 60.) Because a fixed set of rules can be "restrictive," the shared specification of these patents purports to disclose a "dynamic filter" capable of "adding rules to the rule set dynamically" based on information extracted from received packets, such as the port number and IP address. (*See* '612 Patent at 3:1-7, 5:66-6:11.) But this idea was not novel, especially if the claims are expanded beyond the reasonable boundaries of the patent specification by Juniper's litigation-driven claim interpretations.

Dynamic filtering technology was well known before the earliest possible priority date of the '612 patent. For example, the Julkunen reference discloses "[a] dynamic packet filter" that checks packets "on the fly" and creates new rules by extracting source address, destination address and port information from the received packets and attaching an action to apply once a match is found. (Ex. 3 ("Julkunen") at Abstract, 3-4, 18, 21-22.)[2] This dynamically-generated rule is added to the original set of packet-filtering rules and is used by the dynamic packet filter to search for matches in incoming packets. (*Id*. at 13, 21-22.)

[2] "Ex. _" refers to exhibits attached to the Declaration of John C. Mitchell, submitted herewith.

Another problem in the art at the time concerned how to perform additional access filtering in a firewall without decreasing processing speed. (*Compare* '612 Patent at 3:7-9 *with* Ex. 2 ("Bechtolsheim") at 1:28-32 ("One problem in the known art is that processing of packets to enforce access control according to the ACL is processor-intensive and can therefore be relatively slow, particularly in comparison with desired rates of speed for routing packets."); *see also* Mitchell Decl. ¶¶ 69, 96, 98.) The '347 patent allegedly solves this problem by providing a two-step system where a second sorting step follows the firewall engine. ('347 Patent, Fig. 6.) During a first step, the firewall engine sorts packets into "initially allowed packets and initially denied packets." In the second step, the "initially denied packets" are examined further to determine if they should be finally allowed or denied. (*Id.* at 6:60-66.) Once again, under Juniper's broad interpretation of the scope of the claims, using a two-step approach to packet filtering was not a novel idea.

Firewalls with two-step filter technology to reduce processing time were well known before the earliest possible priority date of the '347 patent. For example, Bechtolsheim discloses a first step of sorting packets using access control specifiers that employ rules to associate actions (e.g., allow/deny) with received packets. (Bechtolsheim at Abstract, 1:4-15, 5:10-13, 5:24-31.) The Bechtolsheim system then further sorts these packets in a second step where a priority selector makes the final determination of whether a packet should be allowed or denied. (*See id*. at 2:38-50, 4:48-67, 5:11-19, 7:5-13.)

III. LEGAL STANDARD

To obtain summary judgment, the movant bears the burden of proving that "there is no genuine dispute as to any material fact and [it] is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 585 n.10 (1986). The movant satisfies this burden of proof when no reasonable jury could return a verdict

for the non-moving party. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986). If the movant carries its burden, the nonmovant must then "come forward with specific facts showing that there is a *genuine issue for trial*." *Matsushita*, 475 U.S. at 587 (emphasis in original) (internal quotation marks omitted). To defeat a motion for summary judgment, "[t]he party opposing the motion must point to an evidentiary conflict created on the record at least by a counter statement of a fact or facts set forth in detail in an affidavit by a knowledgeable affiant. Mere denials or conclusory statements are insufficient." *Barmag Barmer Maschinenfabrik AG v. Murata Machinery, Ltd.*, 731 F.2d 831, 835-36 (Fed. Cir. 1984); *see also Matsushita,* 475 U.S. at 586–87 (non-moving party must "do more than simply show that there is some metaphysical doubt as to the material facts"); *Podobnik v. U.S. Postal Service*, 409 F.3d 584, 594 (3d Cir. 2005) (stating party opposing summary judgment "must present more than just bare assertions, conclusory allegations or suspicions to show the existence of a genuine issue") (internal quotation and citation omitted). "If the evidence is merely colorable, or is not significantly probative, summary judgment may be granted." *Anderson*, 477 US at 249-50 (internal citations omitted). The court will "draw all reasonable inferences in favor of the nonmoving party, and it may not make credibility determinations or weigh the evidence." *Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000).

Under 35 U.S.C. § 102, a patent claim is anticipated (and invalid) if "within the four corners of a single, prior art document every element of the claimed invention [is described], either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation." *Callaway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1346 (Fed. Cir. 2009) (quotations and citations omitted). Although the claimed invention needs to be expressly or inherently described, "[t]he prior art need not be ipsissimis verbis (i.e., use identical words as those recited in the claims) to be anticipating." *Cellectis S.A. v. Precision*

Biosciences, Inc., No. 11-173-SLR, 2013 WL 1415609, at *8 (D. Del. Apr. 9, 2013) (citation omitted).

Anticipation requires two steps: (1) construction of the claims and (2) comparison of the construed claims against the alleged prior art. *Key Pharms. v. Hercon Labs. Corp.*, 161 F.3d 709, 714 (Fed. Cir. 1998); *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 147 F.3d 1374, 1378 (Fed. Cir.1998). The allegedly invalid claims are read in context of the corresponding patent specification, and the prosecution history and prior art may also be consulted to assist in determining whether the claimed invention is novel.

Under 35 U.S.C. § 103, a patent claim is obvious if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art. 35 U.S.C. § 103. "Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966)). Although it contains underlying factual inquiries, obviousness is a question of law that may be decided on summary judgment. *Id.*

IV. ARGUMENT

A. Julkunen Anticipates Claims 1, 8, 12-13, 22 and 26-27 and Renders Obvious Claims 4-7 of the '612 Patent

The claimed embodiments of the '612 patent all involve the use of a "dynamic filter" configured to add rules to a set of rules based on "data extracted from" packets. Julkunen explicitly disclosed the use of a "dynamic packet filter" well before the '612 patent was filed.

There can be no genuine dispute that Julkunen's detailed description of this filter anticipates and renders obvious the asserted '612 claims.

1. Overview of Julkunen

The article "*Enhance Network Security with Dynamic Packet Filter*" was authored by Heikki Julkunen and C. Edward Chow in April 1997, and presented at an IEEE conference in 1998. Julkunen is therefore a printed publication that is prior art to the '612 patent.

Julkunen discloses "the study, design and implementation of a firewall" with a "dynamic packet filter." (Julkunen at Abstract.) In Julkunen, this dynamic packet filter is implemented by modifying a standard Linux firewall that uses administrator-programmed rules. (*Id.* at 3-4, 12-14.) Typically, a simple packet filter "only checks the sender/receiver of the packet, and what type of protocol is used" when applying a rule. Julkunen improves the traditional Linux firewall by adding "[a] dynamic packet filter" that checks packets "on the fly." (*Id*. at Abstract.) For example, the Julkunen system can monitor "outgoing IP packets from a computer and then allow[] incoming packets to get through the packet filter if the packets are from the same computer as the outgoing packets were sent to." (*Id*.) The dynamic packet filter creates this new entry by extracting source address, destination address, and port information from the received packets and attaching an action to apply once a match is found. (*Id.* at Abstract, 3-4, 18, 21-22.) This dynamically-generated rule is added to the original set of packet-filtering rules and is used by each packet filter to search for matches in incoming packets. (*Id.* at 13, 21-22.)

Julkunen provides, for example, multiple separate packet filters (abbreviated "PF") that are maintained by the rules. (*Id.* at 13.) These packet filters include:

- Incoming PF. All incoming packets are checked against the rules in the incoming PF chain.
- Forwarding PF. All packets that need to be forwarded are checked against these rules. The packet must pass the incoming PF before it is checked against the rules in the forwarding PF chain.

- Outgoing PF. All outgoing packets are checked against these rules. A packet that is being forwarded has to first pass the forwarding rules, then the outgoing ones.

(*Id.*)

2. Julkunen Is Prior Art to the '612 Patent

On its face, Julkunen states a publication date of April 1997. Juniper therefore cannot (and does not) dispute that Julkunen is a printed publication that was published before April 1, 1999, which is the earliest possible effective filing date of the '612 patent. What Juniper does dispute is whether Julkunen was publicly accessible at the time of its publication. (*See, e.g.*, Ex. 4 ("Stubblebine Rpt.") ¶¶ 722-25.) Juniper's argument lacks merit, however, as public repositories known to those of ordinary skill make clear that Julkunen was presented at the 7th International Conference on Computer Communications and Networks in October 1998, and has been available since at least that date. (Mitchell Decl. ¶¶ 32-36.) Julkunen's accessibility is further evidenced by the fact that it has been cited in other scholarly publications in the same field. (*Id.* ¶ 34.) Thus, Julkunen qualifies as publicly accessible prior art under § 102(a), because it could have been (and was) easily located by "persons interested . . . in the subject matter or art exercising reasonable diligence." *Kyocera Wireless Corp. v. ITC*, 545 F.3d 1340, 1350 (Fed. Cir. 2008) (quotations and citations omitted).

3. Julkunen Discloses the Limitations of the Asserted Independent Claims from the '612 Patent

Juniper asserts independent claims 1, 13, 22 and 27 from the '612 patent. These claims are directed to network devices and methods performed in network devices, which all share the following two core limitations: (1) establishing a set of rules for controlling access to and from a network device for incoming and outgoing data units, and (2) using a dynamic filter to add one or more rules to that set of rules based on data extracted from a sequence of data units. Claim 13 is representative:

13. A network device, comprising:

> an access control engine configured to *establish a set of rules for controlling access to and from the network device for incoming and outgoing data units*; and
>
> a *dynamic filter configured to add one or more first rules to the set of rules based on data extracted from a first sequence of data units* received at the network device.

('612 Patent at 8:61-67 (emphasis added).) Claims 22 and 27 have additional limitations that provide for further filtering and modification of the set of rules. As shown below and in Dr. Mitchell's declaration submitted in support of this motion, Julkunen discloses all of these limitations and therefore anticipates the asserted independent claims. (Mitchell Decl. ¶¶ 140-51, 158-68, 171-76.)

a. Julkunen Discloses Establishing a Set of Rules for Controlling Access

The parties do not dispute that Julkunen discloses establishing a set of rules. Juniper proposes that "rules" should be understood to refer broadly to any type of "if-then" statement. (Juniper's Initial Claim Construction Brief at 9-10.) Julkunen unequivocally discloses the use of a packet filter "that examines the IP packets received and decides if packets are to be forwarded by checking a set of rules that specify what is to happen with the packet." (Julkunen at 3.) In an attempt to create a dispute where none exists, Juniper's expert argues that Julkunen's rules do not satisfy the "rules" limitation in the claims because they supposedly last only for one session. (Stubblebine Rpt. ¶ 729.) But nowhere does Julkunen state that the rules established for its packet filters apply to a single session. Rather, the rules in Julkunen are agnostic as to whether packets belong to a session, and they clearly *do* apply across multiple sessions.

Juniper interprets the term "session" to refer to "a series of packets or communications that are related in some way" (Ex. 12 ("Rubin Rpt.") ¶ 926 fn. 12), which presumably includes packets processed by the same filter. Julkunen's disclosure makes plain that each of the

firewall's multiple packet filters is "maintained by the same rules," though the rules are "applied to packets at different places" (e.g., at the filters for incoming packets, outgoing packets, and/or forwarding packets). (Julkunen at 13-14.) Thus, the same rule would be applied to both packets arriving at the firewall and those leaving the firewall, as well as to those being forwarded to a client within the network. (Mitchell Decl. ¶¶ 65, 142, 146.) The rules in Julkunen apply not only to packets headed in different directions, but also to packets traveling over different ports. (*Id*.) Indeed, Julkunen states that it is possible to make a "rule match a specific port or a range of ports, or up to 10 different ports (counting both source and destination ports) with same rule." (Julkunen at 14.) Because single ports are associated with sessions by those of ordinary skill in the art, this establishes that Julkunen's rules apply across sessions. (Mitchell Decl. ¶¶ 49, 142.)

Moreover, Juniper has clarified that "rules that expressly provide a period of time in which the rule is to be enforced . . . would encompass multiple sessions." (Rubin Rpt. ¶ 959.) The rules in Julkunen operate in this fashion. (Mitchell Decl. ¶ 147.) As the dynamic packet filter inspects packets to see if anything needs to done to the rules, "a timer is updated" on any affected rule, and "as long as the timer value is non-zero the rule is kept." (Julkunen at 18.) For example, when the dynamic filter receives an outgoing packet that does not match a rule, the filter will create a temporal rule regarding incoming packets as well. (*Id.*) This rule "will allow external hosts to send packets to the originator of the packet" without regard to whether the information was requested. (*Id.* at 21 (noting "[t]he temporality of this rule is maintained with a timer").) For example, the dynamic filter of Julkunen can ascertain the port number for a network file system (NFS) connection and generate a rule to allow the connection. (*See, e.g.*, *id.* at 43.) Since the port number for the NFS service does not typically change once registered, such rules will remain in effect across multiple sessions until they are timed out. (*Id.*; Mitchell

Decl. ¶ 149.). Thus, under Juniper's interpretation of the term "session," the rules in Julkunen clearly apply across multiple sessions.

Because the rules in Julkunen are policy-based rules that are distinct from a simple table lookup, Juniper does not dispute that Julkunen discloses rules under PAN's construction of "rule" as well. Thus, there is no genuine dispute that Julkunen discloses establishing a set of rules for controlling access to and from a network device for incoming and outgoing data units.

b. Julkunen Discloses a Dynamic Filter Configured to Add One or More Rules Based on Extracted Data

Juniper cannot (and does not) dispute that Julkunen discloses a dynamic filter. The words "Dynamic Packet Filter" appear in the title of the reference, and even the Abstract states that Julkunen's dynamic filter adds rules by checking packets "on the fly." (Julkunen at 1.) This dynamic filter works exactly as the claims require: when it receives packets that do not have a match to one of its rules, the dynamic packet filter creates a new rule based on data extracted from those packets. (*Id.* at 21 ("If the fivetuple is not matched, an internal DPF [dynamic packet filter] entry is created. When this is done, the DPF will append a temporal rule to the incoming PF [packet filter] as well. The rule in the incoming PF chain will allow external hosts to send packets to the originator of the packet.").) Ultimately, the new rule is added to the existing set of rules, and is applied to incoming and outgoing packets. (Mitchell Decl. ¶¶ 65, 142, 146; *see also* Julkunen at 13 (describing "incoming" and "outgoing" packet as using the same rules), 63 (same).)

As with the previous limitation, Juniper's expert makes a conclusory allegation that the dynamic rules disclosed in Julkunen are limited to one session. (Stubblebine Rpt. ¶¶ 738-41.) To support this allegation, Juniper's expert suggests that Julkunen's dynamic rules are limited to allowing file transfer protocol ("FTP") packets (*id.* ¶ 738), but they are not. Rather, Julkunen

discloses that all packet filters "are maintained by the same rules," and that these rules are applied to incoming, outgoing, and forwarded packets. (Julkunen at 13; *see also id.* at 63 ("the DPF keeps track of both outgoing and incoming packets using the same list of DPF entries"); Mitchell Decl. ¶¶ 65, 142, 146.) If the dynamic packet filter fails to find a match in a particular sequence of outgoing packets that it receives — even if they represent something other than an FTP request — it can create a new rule for use with incoming packets. (Julkunen at 21 (general case), 30 (Telnet), 43 (NFS).) And as established above, the incoming packet filter will apply the rule to all incoming packets, regardless of session. (*See also id.* at 13 ("All incoming packets are checked against the rules in the incoming PF chain."), 21, 63.) Thus, there can be no genuine dispute that Julkunen discloses rules that operate across multiple sessions.

Moreover, Julkunen's FTP example, too, satisfies the requirements of this claim limitation. It was well known in the art that when one computer (the client) establishes an FTP connection to another (the server), the client could provide an address and port that the server then uses to establish a connection back to the client to transmit data using what is called a "PORT command." (Julkunen at 34 ("If data is to be received from the server, a PORT command is sent to the server with the port number to receive data on the client."); Mitchell Decl. ¶ 66.) This second connection back to the client would not be allowed, however, because the firewall would not know the address and port number provided in the command. (Julkunen at 34.) Consequently, incoming packets would be blocked by the filter and the FTP data transfer would fail. (*Id.*; *see also* Mitchell Decl. ¶¶ 66-67.) The '612 patent explicitly sought to solve this problem by providing that dynamic rules can be generated to permit incoming FTP packets after the file transfer request. ('612 Patent at 6:12-27.) Indeed, the specification states that when an "FTP is initiated," the dynamic filter "extracts port number and IP address" from outgoing packets, so it can generate new rules "including these criteria." (*Id.* at 6:12-18.) The

dynamic filter then uses these rules to allow later sequences of incoming FTP packets that would otherwise be denied. (*Id.* at 6:20-21 ("dynamic filter 637 will pass the packets based on the new, dynamically-generated rules").)

The FTP example described in Julkunen works in precisely the same fashion. (Mitchell Decl. ¶ 67.) The dynamic packet filter "scans for the PORT command" in the outgoing packets it receives and "installs appropriate rules," so the return data connection can be established. (Julkunen at 35.) One of ordinary skill would understand that this process involves a rule that applies across multiple sessions because, as shown in the figure below, the incoming packets are received over a different port than that used by the outgoing packets.

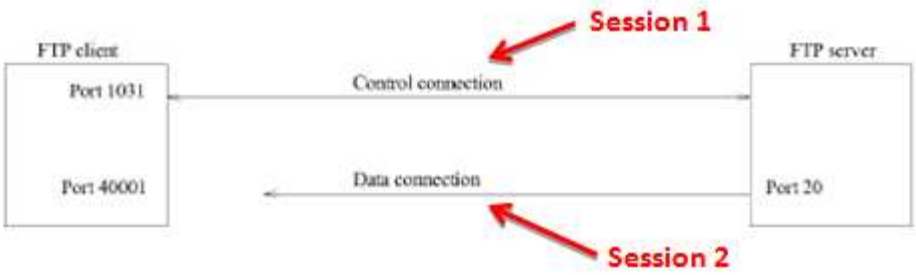

Figure 3.1: FTP port command

(Julkunen at 36 (red arrows and session labels added); *see also* Mitchell Decl. ¶ 67.) The language that the '612 patent's dependent claims use, moreover, makes clear that the patentee intended the independent claims to cover the use of dynamic rules to permit incoming packets after an FTP is initiated. For example, claim 10 depends from claim 1 and provides that the data units extracted from a rule can "comprise file transfer protocol (FTP) data units." ('612 Patent at 8:51-52; *see also id.* at 9:22-24, 10:21-23.) Thus, the rules described in Julkunen's FTP request example apply across multiple sessions as well.

Juniper's expert also makes the unsupported assertion that the rules in Julkunen are not based on data extracted from a "sequence of data units," equating a "data unit" with a packet. (Stubblebine Rpt. ¶¶ 734, 742-44.) But even if the term "data units" does correspond to individual packets, Julkunen discloses this limitation because the filter receives a constant stream of many different types of packets, and uses information extracted from one or more packets in the stream to create new rules. (Julkunen at 21.) While a rule itself may be formed from information in a single packet, this is consistent with how the specification describes rule creation. ('612 Patent at 6:15-16 (describing the extraction of "port number" and "IP address," which is information contained in individual packets).)

c. Julkunen Discloses Filtering Second Data Units Based on the Modified Set of Rules

Claims 22 and 27 require the further step of filtering the second data units based on the modified set of rules. There is no dispute that Julkunen discloses this limitation. Once a new rule is created, Julkunen provides that the rule modifies the complete set of rules and is applied to all packet filters, including the incoming packet filter. (Julkunen at 13, 21, 63; Mitchell Decl. ¶¶ 163-68.) Subsequently, "all incoming packets are checked against the rules." (Julkunen at 13.) This process is the same for any incoming packets. (*Id.*; *see also* Mitchell Decl. ¶¶ 65, 142, 146.)

d. Julkunen Discloses Modifying the First Modified Set of Rules Based on Data Extracted from Second Data Units and Filter Third Data Units Based on Second Modification of the Rules

Claim 27 also requires that the dynamic filter is capable of performing subsequent modifications to the rule set and applying those modifications to received packets. Again, there is no dispute that Julkunen discloses these limitations. According to Julkunen, each time a new rule is established, the set of rules is updated for all the packet filters. (Julkunen at 13, 21-22, 63;

Mitchell Decl. ¶¶ 172-76.) When additional packets are received at a filter, it applies the new rules. (Julkunen at 21; *see also* Mitchell Decl. ¶¶ 65, 142, 146.)

4. Julkunen Discloses the Remaining Elements for Dependent Claims 8, 12, and 26

Dependent claim 8 adds the additional elements of receiving a second sequence of data units and modifying the set of rules based on those data units. Julkunen discloses receiving a second sequence of packets and modifying the set of rules based on the new packets. (*See supra* IV(A)(3)(b).) Julkunen therefore anticipates claim 8. (Mitchell Decl. ¶¶ 152-55.)

Dependent claims 12 and 26 further add the requirement that the data extracted from the sequence of data units comprise a port number and a network address associated with a source of the data units. Juniper does not dispute that Julkunen discloses adding new rules to the packet-filtering rules using source and destination network address and port information extracted from packets. (Stubblebine Rpt. ¶¶ 909-10.) Thus, Julkunen anticipates claims 12 and 26 as well. (Julkunen at 18-22, 43; Mitchell Decl. ¶¶ 156-57, 169-70.)

5. Julkunen in View of NAT Renders Obvious the Remaining Elements for Dependent Claims 4-7

Dependent claims 4 and 5 of the ’612 patent are directed to the basic steps of identifying “network addresses and port numbers associated with source nodes” from which data units in a private network are received, and then replacing them with “a network address and port number associated with the firewall.” (’612 Patent at 8:4-20.) Dependent claims 6 and 7 are directed to the complementary steps of identifying the “network address and port number associated with the firewall” after receiving data units from a public network, and then replacing them with the “network addresses and port numbers associated with corresponding destination nodes” in the private network. (*Id.* at 8:24-41.) This process — called Network Address Translation (“NAT”) — was well-known before the earliest effective filing date of the ’612 patent. (Mitchell Decl. ¶¶

177-87.) When the architecture of the modern Internet was first designed, few if any predicted how popular it would become, so only a limited number of IP addresses were provided in the IP protocol. As the Internet grew, people became concerned that all of the IP addresses might be used up. NAT was developed to allow IP addresses to be reused within private networks, which helped avoid exhaustion of the limited number of IP addresses. (*Id.*)

A person of ordinary skill in the art would have found it obvious to use NAT with the firewall disclosed in Julkunen, because NAT was a standard feature that one of skill would have considered when implementing any firewall to interface between public and private networks at the time of Julkunen's publication. (*Id.*) NAT even solves one of the problems identified by Julkunen — hiding the address information within the private network to improve security — without having to implement a proxy application for the firewall. (Julkunen at 9.) Those ordinarily skilled in the art would therefore have been motivated to add NAT to the Julkunen firewall. *Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1325 (Fed. Cir. 2008) (claim obvious where it was nothing "more than the predictable use of prior art elements according to their established functions"). No technical impediment existed to this combination, as Julkunen describes a Linux-based firewall and Linux implementations for NAT were already known to those of skill in the art. (Mitchell Decl. ¶ 191.) Indeed, during the prosecution of the '612 patent, Juniper neither contested whether a firewall would be combined with NAT functionality nor separately argued whether NAT disclosed the limitations of claims 4-7. ('612 PH, Jan. 3, 2006 Amendment at 20-21 (JA-2345 to -2346) (traverse of rejections to claims 4-7 (originally numbered as claims 24-27) relied only upon arguments as to independent claims).) With the addition of NAT, there is no dispute that the firewall described in Julkunen would satisfy all of the limitations of claims 4-7. (Mitchell Decl. ¶¶ 188-208.) Thus, these claims are rendered obvious by Julkunen in view of NAT.

B. Bechtolsheim Anticipates Claims 1, 14, 16 and 24 of the '347 Patent Under Juniper's Proposed Constructions

The claimed embodiments of the '347 patent are all directed to a two-step process for evaluating packets where the packets are first sorted into "initially allowed packets and initially denied packets." Under Juniper's interpretation of claim limitations at issue, there can be no genuine dispute that Bechtolsheim anticipates the asserted claims from the '347 patent.

1. Overview of Bechtolsheim

U.S. Patent No. 6,377,577 to Bechtolsheim was filed on June 30, 1998, and issued on April 23, 2002. Bechtolsheim is prior art to the '347 patent under 35 U.S.C. § 102(e) because it is a patent granted on an application that was filed in the United States before April 1, 1999, which is the earliest possible effective filing date of the '347 patent. Juniper does not dispute that Bechtolsheim is prior art to the '347 patent. (*See* Stubblebine Rpt. ¶ 603.)

Bechtolsheim is directed to an improved firewall for providing network security by using a two-pass filter system. (Bechtolsheim at 1:4-15.) According to Bechtolsheim, it was well known in the art to control which packets are permitted into and out of a network by using rules within an access control list (ACL). (*Id.* at Abstract, 1:4-15.) Bechtolsheim's ACL is composed of a sequence of access control entries, which are if/then statements for how to treat a packet if a match is found. (*Id.* at 5:10-13, 5:24-31 ("Access control entries can specify that particular actions are permitted, denied, or that they will be recorded in a log.").) Access control specifiers map to the access control entries, and are used to filter incoming packets. (*Id.* at 5:10-13.) Each access control specifier that matches a packet associates a rule that permits or denies access for that packet. (*Id.*; *see also id.* at 4:48-67.) Bechtolsheim discloses that a priority selector — which is also referred to as a priority encoder — then takes outputs from the access control specifiers and chooses the action that should be taken. (*Id.* at 2:44-47 ("Successful matches are input to a priority selector, which selects the match with the highest priority.").)

2. Bechtolsheim Discloses the Limitations of the Asserted Independent Claims from the '347 Patent Under Juniper's Proposed Constructions

The asserted independent claims 1, 14 and 24 from the '347 patent are directed to a firewall apparatus and methods performed in a firewall that use a two-step process: (1) sorting incoming packets into initially allowed and initially denied packets, and (2) further sorting the initially denied packets into allowed packets and denied packets. Claim 14 is representative:

> 14. A method for providing network computer security, comprising:
>
> receiving incoming packets at a firewall;
>
> *sorting the incoming packets into initially allowed packets and initially denied packets*; and
>
> *further sorting the initially denied packets into allowed and denied packets* using rules.

('347 Patent at 8:11-17 (emphasis added).) If the Court adopts Juniper's interpretation of "initially denied" — which includes the mere association of a packet with a rule that could result in a denial — Bechtolsheim clearly discloses this two-step process. As shown below and in Dr. Mitchell's declaration, Bechtolsheim therefore anticipates these claims. (Mitchell Decl. ¶¶ 101-21, 130-34.)

a. Bechtolsheim Discloses Sorting Incoming Packets Into Initially Allowed and Initially Denied Packets

Claims 1, 14 and 24 each require the step of processing incoming packets by sorting them into initially allowed and initially denied packets. Although Juniper suggests that "initially denied" need not be construed, Juniper nevertheless contends this term *does not* require that a packet "be identified to be dropped." (Juniper's Initial Claim Construction Brief at 12.) Indeed, Juniper's infringement expert states that a packet is "initially denied" by virtue of being "associated" with a rule that could result in a "deny" action, even if that action is never assigned

to the packet. (Rubin Rpt. ¶ 847.) PAN disagrees with Juniper's interpretation, but if the Court agrees with Juniper, then there is no dispute that Bechtolsheim discloses this limitation.

Bechtolsheim describes an "access control memory" that contains access control specifiers, each of which is mapped to an access control entry. (Bechtolsheim at 4:34-36, 5:11-19, Fig 2.) These access control entries are rules under either party's construction of "rule," because they include information that the access control specifiers use to search for matching criteria in incoming packets (not using a lookup table), and if a match is found for the packet, the rules describe what action to take for that packet. (*Id*. at 1:16-20, 5:11-19, 9:4-8; Mitchell Decl. ¶¶ 97, 107-08.) The structure of the access control entry explicitly provides for an allow/deny decision for each rule match. (Bechtolsheim at 5:11-19, 5:25-26 ("[a]ccess control entries can specify that particular actions are permitted, denied, or that they will be recorded in a log").) Thus, when incoming packets match an access control entry with a "deny" action, they have been sorted into "initially denied packets" under Juniper's interpretation of that term. (Mitchell Decl. ¶ 108.)

To rebut the position that Bechtolsheim's access specifiers sort packets into "initially allowed packets and initially denied packets," Juniper's expert relies on an interpretation similar to PAN's proposed construction of "initially denied." Indeed, Juniper's expert argues that the comparison of packets to access control specifiers "*does not itself determine any disposition of a packet*," so this comparison does not sort packets into "initially allowed packets and initially denied packets." (Stubblebine Rpt. ¶ 607 (emphasis in original).) If the first step in the claimed sorting packets process requires a firewall to make a "*determination as to disposition of a packet*" as Juniper's expert says it must (*id.*), then PAN's construction is correct and PAN would not infringe the asserted '347 patent claims. If, by contrast, Juniper's interpretation of the claims is adopted by the Court, then Bechtolsheim would satisfy this claim limitation.

b. Bechtolsheim Discloses Further Sorting the Initially Denied Packets into Allowed Packets and Denied Packets

Claims 1, 14 and 24 each require a second processing step of further sorting the initially denied packets into allowed packets and denied packets. Bechtolsheim discloses a "priority selector" that uses a second set of rules to process the packets that matched the access control entries. (Bechtolsheim at 4:48-51, 7:5-11, 2:44-47 ("Successful matches are input to a priority selector, which selects the match with the highest priority (that is, the match that is first in the sequence of access control specifiers).").) The priority selector makes the final determination as to which action (allow/deny) will be applied to each packet by selecting the access control specifier with highest priority. (*Id.* at 4:51-67.) Thus, as shown in the figure below, the priority selector/encoder sorts some "initially denied" packets into finally allowed or denied packets.

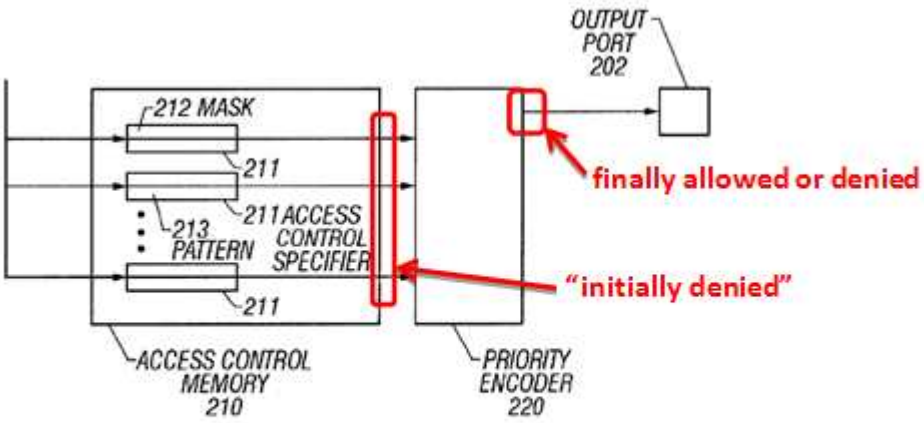

FIG. 2

(*Id.*, Fig. 2 (red arrows and allowed/denied labels added); Mitchell Decl. ¶ 112.)

Juniper's expert suggests that Bechtolsheim's "priority selector" uses the same set of rules as the access control specifiers (Stubblebine Rpt. ¶¶ 614, 616), but this is clearly not the case. Rather, the priority selector determines which access control specifier has priority based not on the access control entry rules, but instead on a separate set of priority rules for finalizing

the determination made by matching packets to access control entries. (Bechtolsheim at 2:44-47; Mitchell Decl. ¶¶ 100, 110-11.) Indeed, the whole purpose behind the invention disclosed in Bechtolsheim was to move the final priority determinations until after the initial match determinations are made. (Bechtolsheim at 2:38-50, 5:11-19; 7:34-48; Mitchell Decl. ¶¶ 98-100.) Therefore, the rules for the priority selector cannot be the same set of rules as those for the access control specifiers.

Juniper also contends that the priority rules used by the priority selector are not even rules at all. But to make this argument, Juniper relies on *PAN's* proposed construction of "rule," which requires that a rule be "a policy for filtering packets." (*Compare* Stubblebine Rpt. ¶ 617, *with* PAN's Claim Construction Brief at 24-27.) Juniper does not even argue whether Bechtolsheim discloses "rules" under its own construction. But Juniper clearly cannot interpret the claims one way for infringement and another way for invalidity. *Source Search Techs., LLC v. LendingTree, LLC*, 588 F.3d 1063, 1075 (Fed. Cir. 2009) ("Claims may not be construed one way in order to obtain their allowance and in a different way against accused infringers.") (citation and quotations omitted).

Juniper's expert also suggests that the priority selector does not further sort "initially denied" packets because it reviews all packets processed by the access control specifiers regardless of whether they were initially denied or allowed. (Stubblebine Rpt. ¶ 615.) But Juniper cannot point to any support in the asserted claims explicitly requiring that *only* "initially denied packets" can receive further sorting. In short, there is no genuine dispute that Bechtolsheim anticipates the asserted independent claims under Juniper's interpretation of "initially denied" and "rule."

3. Bechtolsheim Discloses Additional Elements in Dependent Claim 16

Bechtolsheim also discloses the following additional limitations found in dependent claim 16: (1) sorting the incoming packets by using fixed rules and (2) further sorting the initially allowed packets into allowed packets and packets requiring modification. (Mitchell Decl. ¶¶ 122-26.)

a. Bechtolsheim Discloses Sorting the Incoming Packets Using Fixed Rules

Dependent claim 16 requires and Bechtolsheim discloses the step of sorting incoming packets using fixed rules. According to Bechtolsheim, the access control specifiers "are recorded in a CAM (content-addressable memory)," which are hardware circuits designed to detect a particular match between the packets to which the rule applies and the incoming packet. (Bechtolsheim at Abstract ("The invention provides for hardware processing of ACLs and thus hardware enforcement of access control."), 2:51-54 ("an array of ternary elements for matching on logical '0', logical '1', or on any value, and each of which generates a match signal."); Mitchell Decl. ¶ 124.) The patterns that each access control specifier can match are preset. (*See, e.g.*, Bechtolsheim at 4:34-43, 5:66-6:9.) Accordingly, Bechtolsheim discloses access control entries that are fixed rules used by the hardware based access control specifiers. (Mitchell Decl. ¶¶ 124-25.)

b. Bechtolsheim Discloses Further Sorting the Initially Allowed Packets into Allowed Packets and Packets Requiring Modification

Bechtolsheim also discloses the step in dependent claim 16 of further sorting the initially allowed packets into allowed packets and packets requiring modification. Bechtolsheim's priority selector reviews all of the initial determinations (allow, deny, and further processing) on a packet, assesses priority, and finalizes them as a final determination either to allow, deny, or

pass the packet for further processing. (Bechtolsheim at 4:48-67; Mitchell Decl. ¶¶ 100, 110-12.) Bechtolsheim further discloses routing IP packets that have been allowed. (*See, e.g.*, Bechtolsheim at 3:1-4; *see also id.* at 8:6-9; Mitchell Decl. ¶ 129.) It also would have been understood by a person having ordinary skill in the art that IP packets include a time-to-live value, and routing a packet necessarily requires modifying the time-to-live value, because the time-to-live value is a part of an IP packet and it must be updated as the packet passes through each network node. (Mitchell Decl. ¶ 129.)

V. CONCLUSION

The prior art discloses the limitations of the '612 and '347 patents under Juniper's broad reading of the scope of the asserted claims. The Court should therefore grant summary adjudication that both patents are anticipated and rendered obvious.

POTTER ANDERSON & CORROON LLP

OF COUNSEL:

Harold J. McElhinny
Michael A. Jacobs
Matthew I. Kreeger
Matthew A. Chivvis
Morrison & Foerster LLP
425 Market Street
San Francisco, CA 94105-2482
(415) 268-7000

Daralyn J. Durie
Ryan M. Kent
Durie Tangri LLP
217 Leidesdorff Street
San Francisco, CA 94111
(415) 362-6666

By: */s/ Philip A. Rovner*
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

Attorneys for Defendant
Palo Alto Networks, Inc.

Dated: August 20, 2013
1119658

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, Philip A. Rovner, hereby certify that on August 20, 2013 the within document was electronically filed with the Clerk of the Court using CM/ECF which will send notification to the registered attorney(s) of record that the document has been filed and is available for viewing and downloading.

I further certify that on August 20, 2013, the within document was served on the following persons as indicated:

BY E-MAIL

Jack B. Blumenfeld, Esq.
Jennifer Ying, Esq.
Morris, Nichols, Arsht & Tunnel LLP
1201 N. Market Street
P.O. Box 1347
Wilmington, DE 19899
jblumenfeld@mnat.com
jying@mnat.com

BY E-MAIL

Morgan Chu, Esq.
Jonathan S. Kagan, Esq.
Irell & Manella LLP
1800 Avenue of the Stars
Suite 900
Los Angeles, CA 90067-4276
mchu@irell.com
jkagan@irell.com

Lisa S. Glasser, Esq.
David C. McPhie, Esq.
Rebecca Clifford, Esq.
Mytili Bala, Esq.
Irell & Manella LLP
840 Newport Center Drive, Suite 400
Newport Beach, CA 92660
lglasser@irell.com
dmcphie@irell.com
rclifford@irell.com
mbala@irell.com

/s/ Philip A. Rovner
Philip A. Rovner (#3215)
Potter Anderson & Corroon LLP
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com